1 **Listing of Claims:**

2 What is claimed, is

3 1. (Currently Amended) A method for providing a user device with a set of access codes, the
4 method comprising:
5   in the user device, storing an encryption key and an identification code, and sending a
6 message containing the identification code to a server via a communications network;
7   in the server, storing an encryption key corresponding to the key stored in the user device,
8 allocating the set of access codes on receipt of the identification code from the user device,
9 performing a look up function based on the identification code received in the message to retrieve
10 the key from storage, encrypting the set of access codes using the retrieved key to produce an
11 encrypted set, and sending a message containing the encrypted set to the user device via the
12 network;
13   in the user device, decrypting the encrypted set received from the server using the key in
14 storage, and storing the decrypted set of access codes for use by a user of the user device; and,
15   upon the number of unused access codes reaching a predetermined threshold, in the
16 server, sending a message containing a new set of access codes to the user device via the network;
17
18   in the user device, storing the new set for use by a user of the user device; and

19 selectively:
20   in the user device, tracking the access codes used by the user, generating a request in
21 response to the number of unused access codes reaching a predetermined threshold, and sending a
22 message containing the request to the server; and
23   in the server, sending the message containing the new set of access codes on receipt of the
24 request; or

1   in the server, tracking the access codes used by the user, and sending the message

2   containing the new set of access codes to the user device in response to the number of unused

3   access codes reaching a predetermined threshold; or

4   in the server, generating a new key, encrypting the new key with the previous key, and

5   sending a message containing the encrypted new key to the user device via the network; and, in

6   the user device, decrypting the new key received from the server using the previous key, and

7   storing the decrypted new key in place of the previous key; or

8   in the server, encrypting a new set of access codes with the new key to produce a new key

9   encrypted set, and sending a message containing the new key encrypted set to the user device via

10   the network, and,

11   in the user device, decrypting the new key encrypted set using the new key, and storing

12   the decrypted new set for use by a user of the user device; or

13   in the user device, generating a public/private key pair, and sending a message containing

14   the public key of the pair to the server via the network,

15   in the server, generating a session key, encrypting the set of access codes with the session

16   key to produce a session key encrypted set, encrypting the session key with the public key to

17   produce an encrypted session key, sending a message containing the session key encrypted set and

18   the encrypted session key to the user device via, the network, and,

19   in the user device, decrypting the encrypted session key with the private key of the pair to

20   recover the session key, decrypting the session key encrypted set with the recovered session key

21   to recover the set, and storing the decrypted set for use by a user of the user device.

22   2. - 41. (Canceled)

23